In the Claims

Please amend claims 18 and 26 as indicated below:

1. **(ORIGINAL)** A Web server input string screening method comprising:

determining an attack pattern that can be used to attack a Web server;

defining a search pattern that can be used to detect the attack pattern, the search pattern being defined in a manner that permits variability among its constituent parts;

receiving an input string that is intended for use by a Web server;

evaluating the input string using the search pattern to ascertain whether the attack pattern is present; and

implementing a remedial action if an attack pattern is found that matches the search pattern.

2. **(ORIGINAL)** The Web server input string screening method of claim 1, wherein:

said defining comprises defining a plurality of different search patterns; and

said evaluating comprises evaluating the input string using said plurality of different search patterns.

3. **(ORIGINAL)** The Web server input string screening method of claim 1, wherein the search pattern is specified as a regular expression.

4. **(ORIGINAL)** The Web server input string screening method of claim 1, wherein said receiving of the input string comprises receiving a URL.

5. **(ORIGINAL)** The Web server input string screening method of claim 1, wherein said receiving of the input string comprises receiving a portion of an HTTP verb request.

6. **(ORIGINAL)** The Web server input string screening method of claim 1, wherein said implementing comprises denying a request that is associated with the input string.

7. **(ORIGINAL)** A Web server input string screening method comprising:

defining one or more search patterns that comprise literal characters and special characters, wherein the literal characters indicate exact characters in an input string that is intended for receipt by a Web server, and the special characters indicate variable characters in an input string that is intended for receipt by the Web server, the search patterns being usable to search for an attack pattern that can be used to attack the Web server; and

storing the one or more search patterns in a memory location that is accessible to a screening tool for evaluating an input string that is intended for receipt by the Web server.

8. **(ORIGINAL)** The Web server input string screening method of claim 7 further comprising:

retrieving a search pattern from the memory location; and evaluating an input string with the screening tool by ascertaining whether the input string includes at least a portion that matches the search pattern.

9. **(ORIGINAL)** The Web server input string screening method of claim 8, wherein the evaluating of the input string comprises evaluating a URL.

10. **(ORIGINAL)** The Web server input string screening method of claim 8, wherein the evaluating of the input string comprises evaluating a portion of an HTTP verb request.

11. **(ORIGINAL)** The Web server input string screening method of claim 7 further comprising implementing the screening tool as an extension for an existing Web server.

12. **(ORIGINAL)** The Web server input string screening method of claim 7 further comprising implementing the screening tool as an ISAPI extension.

13. **(ORIGINAL)** A Web server input string screening method comprising:

defining one or more search patterns that are specified as a regular expression, the search patterns being usable to search for an attack pattern that can be used to attack the Web server; and

storing the one or more search patterns in a memory location that is accessible to a screening tool for evaluating an input string that is intended for receipt by the Web server.

14. **(ORIGINAL)** The Web server input string screening method of claim 13 further comprising:

retrieving a search pattern from the memory location; and

evaluating an input string with the screening tool by ascertaining whether the input string includes at least a portion that matches the search pattern.

15. **(ORIGINAL)** The Web server input string screening method of claim 14, wherein the evaluating of the input string comprises evaluating a URL.

16. **(ORIGINAL)** The Web server input string screening method of claim 14, wherein the evaluating of the input string comprises evaluating a portion of an HTTP verb request.

17. **(ORIGINAL)** A computer-readable medium having computer-readable instructions thereon which, when executed by a computer, perform the method of claim 14.

18. **(CURRENTLY AMENDED)** A Web server input string screening tool embodied on a computer-readable medium comprising:

a pattern matching engine that is configured to receive an input string that is intended for use by a Web server and evaluate the input string to ascertain whether it likely constitutes an attack on the Web server; and one or more patterns that are usable by the pattern matching engine to evaluate the input string, the patterns being defined in a manner that permits variability among the constituent parts of the one or more patterns.

19. **(ORIGINAL)** The Web server input string screening tool of claim 18, wherein the one or more patterns are specified as regular expressions.

20. **(ORIGINAL)** The Web server input string screening tool of claim 18, wherein the pattern matching engine is configured to receive an input string that comprises a URL.

21. **(ORIGINAL)** The Web server input string screening tool of claim 18, wherein the pattern matching engine is configured to receive an input string that comprises a portion of an HTTP verb request.

22. **(ORIGINAL)** One or more computer readable media having computer-readable instructions thereon which, when executed by a computer perform the following steps:

receiving an input string that is intended for use by a Web server;

evaluating the input string using a search pattern to ascertain whether the input string contains an attack pattern that can be used to attack the Web server, the search pattern comprising literal characters and special characters, wherein literal characters indicate exact characters in the input string, and the special characters indicate variable characters in the input string; and implementing a remedial action if an attack pattern is found that matches the search pattern.

23. **(ORIGINAL)** The computer-readable media of claim 22, wherein said implementing comprises denying a request that is associated with the input string.

24. **(ORIGINAL)** The computer-readable media of claim 22, wherein said receiving comprises receiving a URL.

25. **(ORIGINAL)** The computer-readable media of claim 22, wherein said receiving comprises receiving an input string that is associated with an HTTP verb request.

26. **(CURRENTLY AMENDED)** A collection of Web server screening patterns embodied on a computer-readable medium comprising:

a memory; and

a plurality of attack patterns stored in the memory, the attack patterns being useable to screen input strings that are intended for use by a Web server, individual attack patterns being defined in a manner that permits variability among their constituent parts.

27. **(ORIGINAL)** The collection of claim 26, wherein the patterns are specified as regular expressions.

28. **(ORIGINAL)** The collection of claim 26, wherein the collection is adapted for addition to, deletion of, or modification of patterns.

29. **(ORIGINAL)** The collection of claim 26, wherein the patterns are configured for use in screening URLs that are intended for use by a Web server.

30. **(ORIGINAL)** The collection of claim 26, wherein the patterns are configured for use in screening input strings associated with HTTP verb requests that are intended for use by a Web server.

31. **(ORIGINAL)** The collection of claim 26 configured for use by an ISAPI extension.